

①9 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

①1 N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

2 795 897

②1 N° d'enregistrement national : **99 08394**

⑤1 Int Cl⁷ : H 04 L 12/22, G 07 F 7/08, H 04 Q 7/20

⑫

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 30.06.99.

③0 Priorité :

④3 Date de mise à la disposition du public de la
demande : 05.01.01 Bulletin 01/01.

⑤6 Liste des documents cités dans le rapport de
recherche préliminaire : *Se reporter à la fin du
présent fascicule*

⑥0 Références à d'autres documents nationaux
apparentés :

⑦1 Demandeur(s) : SCHLUMBERGER SYSTEMES
Société anonyme — FR.

⑦2 Inventeur(s) : GUION CHRISTIAN et CHERIFI
OMAR.

⑦3 Titulaire(s) :

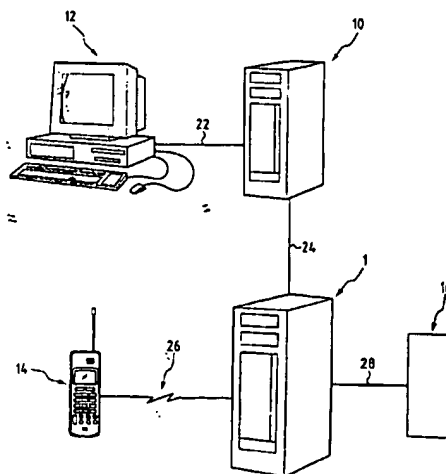
⑦4 Mandataire(s) : CABINET BEAU DE LOMENIE.

⑤4 PROCÉDE ET DISPOSITIF DE TRANSACTION SECURISEE SUR RESEAU.

⑤7 L'invention propose un procédé de transaction sécurisée sur réseau, un utilisateur ayant envoyé à un serveur web (10) des données d'identification personnelles et une commande en entrant lesdites données d'identification personnelles et ladite commande sur un ordinateur (12), le serveur web (10) ayant transmis lesdites données d'identification personnelles et ladite commande à un dispositif de transaction sécurisée (1), l'utilisateur étant répertorié auprès d'un organe de paiement (16), comportant les étapes suivantes:

on demande confirmation à l'utilisateur de la transaction par voie hertzienne (26), et

on transmet l'information de confirmation de la transaction au serveur web (10) et à l'organe de paiement (16).



FR 2 795 897 - A1



L'invention concerne un procédé et un dispositif de transaction sécurisée sur réseau.

Des transactions sont effectuées sur des réseaux notamment sur le réseau Internet par des utilisateurs. Ainsi, un utilisateur consultant les pages d'un serveur web accessible sur le réseau Internet peut effectuer des transactions telles que l'achat d'articles proposés sur ledit serveur web. L'utilisateur peut ainsi passer une commande et conclure la transaction. Pour payer, l'utilisateur donne en général son numéro de carte bancaire qui est véhiculé sur le réseau.

De telles transactions appelées transactions électroniques ne sont pas sécurisées, ainsi des données telles que le numéro de carte bancaire circulant sur le réseau peuvent être interceptées par un tiers et être utilisées à des fins préjudiciables pour le titulaire de la carte.

On connaît des procédés et des dispositifs pour sécuriser les transactions électroniques, mais ces procédés et ces dispositifs nécessitent l'utilisation de moyens annexes spécifiquement prévus pour la transaction : on connaît ainsi par exemple des lecteurs pour ordinateur prévus pour des cartes, des moyens cryptologiques dans l'ordinateur ou dans le lecteur. Il existe plusieurs standards.

L'invention propose un procédé et un dispositif judicieux permettant de simplifier la sécurisation des transactions électroniques. L'invention a également pour objet de rendre cette sécurisation plus sûre et moins coûteuse.

Plus précisément l'invention propose un procédé de transaction sécurisée sur réseau, ledit réseau comprenant au moins un serveur web à disposition d'un utilisateur et un dispositif de transaction sécurisé, caractérisé en ce qu'il comporte les étapes suivantes :

- on transmet des données d'identification personnelles ainsi qu'une demande de transaction de l'utilisateur au dispositif de transaction sécurisé, par l'intermédiaire du serveur web,

- on demande confirmation à l'utilisateur de la demande de transaction par voie hertzienne, et
- on transmet l'information de confirmation de la transaction au serveur web.

5 Avantageusement, la demande de confirmation par voie hertzienne et la transmission de l'information de confirmation se font au moyen du dispositif de transaction sécurisé.

De préférence, on confirme la transaction à l'utilisateur.

Avantageusement, l'information de confirmation de la transaction
10 envoyée à un organe de paiement comporte un message de débit.

De préférence, les données d'identification personnelles comportent des données telles que numéro d'abonné ou numéro de téléphone à l'exclusion d'un numéro de carte bancaire.

Avantageusement, le dispositif de transaction sécurisée est un
15 serveur de téléphonie mobile.

De préférence, on archive la transaction.

Avantageusement, l'utilisateur étant répertorié auprès d'un organe de paiement, on transmet l'information de confirmation à l'organe de paiement.

L'invention propose également un dispositif de transaction sécurisée
20 sur réseau, ledit réseau comprenant au moins un serveur web à disposition d'un utilisateur, caractérisé en ce qu'il comporte des moyens pour recevoir une demande de transaction et des données d'identification personnelles de l'utilisateur, des moyens pour demander confirmation par voie hertzienne à l'utilisateur de la demande de transaction, et, des moyens de transmission
25 de l'information de confirmation au serveur web.

De préférence, le dispositif comporte des moyens de confirmation de la transaction à l'utilisateur.

Avantageusement, l'information de confirmation de la transaction envoyée à un organe de paiement comporte un message de débit.

De préférence, le dispositif de transaction sécurisée est un serveur de téléphonie mobile.

Avantageusement, le dispositif comporte un moyen d'archivage la transaction.

- 5 De préférence, l'utilisateur étant répertorié auprès d'un organe de paiement, le dispositif comporte des moyens de transmission de l'information de confirmation à l'organe de paiement.

- D'autres caractéristiques et avantages de l'invention apparaîtront au cours de la description d'un mode de réalisation qui va suivre, donné à titre
10 d'exemple non limitatif, à l'appui de la figure sur laquelle est représenté un dispositif de transaction sécurisée.

- Un dispositif de transaction sécurisée 1 qui est un serveur GSM est relié à un serveur web 10 par une connexion par câble 24. Un tel serveur GSM est bien connu pour l'homme de l'art et n'est pas décrit ici. Le serveur
15 web 10 est relié au réseau Internet. Un utilisateur est installé devant une station qui est un ordinateur personnel 12 connecté via le réseau Internet au site web 10. Cette connexion par câble porte la référence 22 (figure). L'utilisateur dispose d'un téléphone mobile 14 relié au dispositif de transaction sécurisée 1 par une connexion par voie hertzienne 26.
- 20 L'utilisateur est répertorié auprès d'une banque 16 où il a un compte. La banque 16 est reliée au dispositif de transaction sécurisée 1 par un lien 28 tel qu'un réseau de communications ou télécommunications d'un type connu.

- Un procédé de transaction sécurisée va maintenant être décrit.
- 25 L'utilisateur consulte sur son ordinateur personnel 12 une page du serveur web 10 sur laquelle on lui propose d'acheter un article. L'utilisateur qui veut acheter l'article envoie au serveur web 10 des données d'identification telles que son numéro de téléphone portable ou son numéro d'abonné : pour ce faire l'utilisateur tape les données sur l'ordinateur personnel 12 et les
30 transmet via le réseau Internet au serveur web 10. On note que ce faisant,

l'utilisateur n'envoie pas de données que l'on pourraient qualifier de sensibles telles qu'un numéro de carte bancaire.

Le serveur web 10 interroge via le câble 24 le dispositif de transaction sécurisée 1 pour connaître l'authenticité des données
5 d'identification de l'utilisateur.

Si les données d'identification sont concordantes, le dispositif de transaction sécurisée 1 approuve l'identité de l'utilisateur et transmet l'approbation au serveur web 10. Le serveur web 10 permet alors à l'utilisateur de commander l'article qu'il veut acheter.

10 L'utilisateur envoie, au serveur web 10, un code spécial pour la transaction correspondant à un numéro de compte bancaire par exemple.

Le serveur web 10 envoie un message contenant une information de transaction intégrant le code spécial et l'objet de l'achat (par exemple le prix de l'article, sa désignation, sa référence, l'heure et la date d'achat) et envoie
15 cette information au serveur de transaction sécurisée 1 via le câble 24.

Le message envoyé est au format connu sous la désignation "sms". Le format "sms" est défini dans la norme du GSM, connue sous le nom "norme GSM 11.11 de l'ETSI".

Le dispositif de transaction sécurisée 1 demande confirmation à
20 l'utilisateur de l'achat par la connexion par voie hertzienne 26 en le contactant sur le téléphone mobile 14, en envoyant audit téléphone mobile 14 un message intégrant l'objet de l'achat. Après avoir vérifié l'objet de l'achat sur son téléphone mobile 14, l'utilisateur confirme la transaction au serveur de transaction sécurisée 1 au moyen du téléphone mobile 14.

25 Le dispositif de transaction sécurisée 1 confirme l'achat au serveur web 10.

Le dispositif de transaction sécurisée 1 archive la transaction et transmet un ordre de payer en envoyant un message de débit à la banque 16 via le lien 28 et de crédit au serveur web 10 via le câble 24.

Le dispositif de transaction sécurisée 1 confirme le débit à l'utilisateur en envoyant un message sur le téléphone mobile 14.

Selon une variante, l'utilisateur envoie simultanément au serveur web 10 à la fois les données d'identification de l'utilisateur et la commande avec
5 le code spécial.

Selon une autre variante plus avantageuse, lorsque l'utilisateur confirme la transaction au serveur de transaction 1 au moyen de son téléphone mobile, il envoie également le code spécial correspondant par exemple à un numéro de compte bancaire. Ainsi le code spécial n'est plus
10 envoyé via le serveur web, ce qui sécurise d'autant plus la transaction.

Bien entendu, la présente invention n'est nullement limitée au mode d'exécution décrit et représenté qui n'a été donné qu'à titre d'exemple. En particulier, elle comprend tous les moyens constituant des équivalents techniques des moyens décrits ainsi que leurs combinaisons, si celles-ci
15 sont exécutées selon l'esprit de l'invention.

REVENDICATIONS

1. Procédé de transaction sécurisée sur réseau, ledit réseau comprenant au moins un serveur web (10) à disposition d'un utilisateur et
5 un dispositif de transaction sécurisé, caractérisé en ce qu'il comporte les étapes suivantes :

- on transmet des données d'identification personnelles ainsi qu'une demande de transaction de l'utilisateur au dispositif de transaction sécurisé (1), par l'intermédiaire du serveur web (10),
- 10 - on demande confirmation à l'utilisateur de la demande de transaction par voie hertzienne (26), et
- on transmet l'information de confirmation de la transaction au serveur web (10).

2. Procédé selon la revendication 1, caractérisé en ce que la
15 demande de confirmation par voie hertzienne et la transmission de l'information de confirmation se font au moyen du dispositif de transaction sécurisé (1).

3. Procédé selon l'une quelconque des revendications 1 ou 2, caractérisé en ce qu'on confirme la transaction à l'utilisateur.

20 4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que l'information de confirmation de la transaction envoyée à un organe de paiement comporte un message de débit.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que les données d'identification personnelles comportent
25 des données telles que numéro d'abonné ou numéro de téléphone à l'exclusion d'un numéro de carte bancaire.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que le dispositif de transaction sécurisée est un serveur de téléphonie mobile.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'on archive la transaction.

8. Procédé selon l'une quelconque des revendications 1 à 7, l'utilisateur étant répertorié auprès d'un organe de paiement (16),
5 caractérisé en ce que on transmet l'information de confirmation à l'organe de paiement (16).

9. Dispositif de transaction sécurisée sur réseau, ledit réseau comprenant au moins un serveur web (10) à disposition d'un utilisateur, caractérisé en ce qu'il comporte des moyens pour recevoir une demande de
10 transaction et des données d'identification personnelles de l'utilisateur, des moyens pour demander confirmation par voie hertzienne (26) à l'utilisateur de la demande de transaction, et, des moyens de transmission de l'information de confirmation au serveur web (10).

10. Dispositif selon la revendication 9, caractérisé en ce qu'il
15 comporte des moyens de confirmation de la transaction à l'utilisateur.

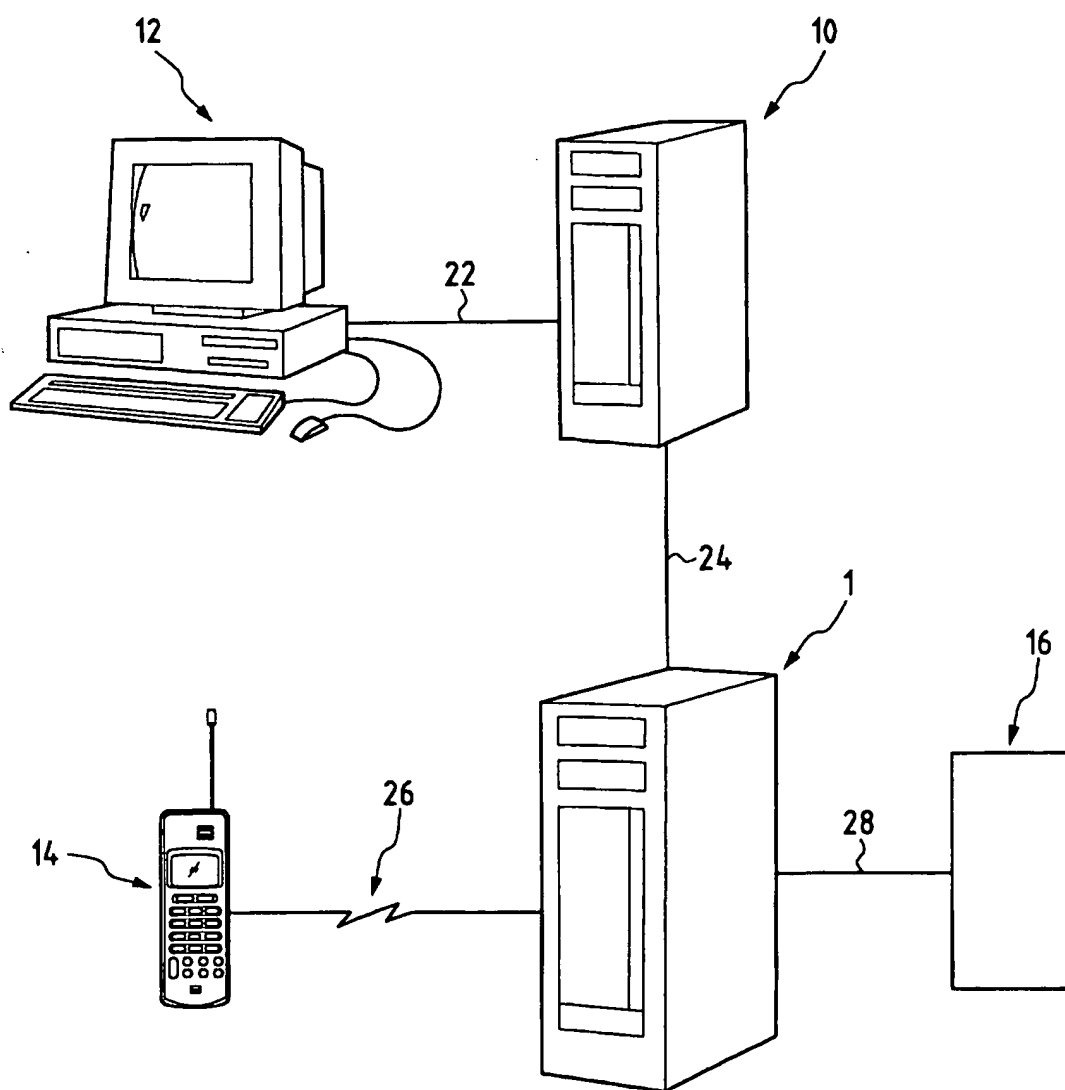
11. Dispositif selon la revendication 9 à 10, caractérisé en ce que l'information de confirmation de la transaction envoyée à un organe de paiement comporte un message de débit.

12. Dispositif selon l'une quelconque des revendications 9 à 11,
20 caractérisé en ce que le dispositif de transaction sécurisée est un serveur de téléphonie mobile.

13. Dispositif selon l'une quelconque des revendications 9 à 12, caractérisé en ce qu'il comporte un moyen d'archivage la transaction.

14. Dispositif selon l'une quelconque des revendications 9 à 13,
25 l'utilisateur étant répertorié auprès d'un organe de paiement (16), caractérisé en ce qu'il comporte des moyens de transmission de l'information de confirmation à l'organe de paiement (16).

1/1



INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

**RAPPORT DE RECHERCHE
PRELIMINAIRE**
établi sur la base des dernières revendications
déposées avant le commencement de la recherche

N° d'enregistrement
national

FA 577675
FR 9908394

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	NL 1 007 409 C (NEDERLAND PTT) 18 novembre 1997 (1997-11-18)	1,2,6,9, 12
Y	* page 1, ligne 28 - page 2, ligne 15; figure 1 *	3,5,7,8, 10,13,14
X	US 5 668 876 A (FALK JOHAN PER ET AL) 16 septembre 1997 (1997-09-16) * abrégé * * colonne 1, ligne 65 - colonne 2, ligne 26 * * colonne 3, ligne 14 - ligne 50 * * colonne 5, ligne 22 - ligne 34 * * colonne 6, ligne 55 - colonne 7, ligne 48 * * figures 1,2 *	1,6,9
Y	US 5 903 721 A (SIXTUS TIMOTHY) 11 mai 1999 (1999-05-11)	3,5,8, 10,14 4,11
A	* colonne 3, ligne 10 - ligne 25 * * colonne 4, ligne 65 - colonne 5, ligne 27 * * colonne 6, ligne 65 - colonne 7, ligne 53 * * colonne 8, ligne 35 - ligne 47 * * colonne 9, ligne 25 - ligne 32 * * figures 1,2 *	
Y	US 5 715 314 A (MACKIE DAVID J ET AL) 3 février 1998 (1998-02-03) * colonne 3, ligne 38 - ligne 56 *	7,13
Date d'achèvement de la recherche		Examineur
1 mars 2000		Blanco Cardona, P
<p>CATEGORIE DES DOCUMENTS CITES</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou antérie-plan technologique général O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons</p> <p>& : membre de la même famille, document correspondant</p>		